Defence Children Services

DCS Directive 7.1.2

Records Management

DCS May 19 v1.0

General

Authorisation	Director DCS
Senior Responsible Owner	
Point of Contact	01980 61 XXXX
Review Date	XXX 20XX
Related Policy/Guidance	
DPA 2018	Data Protection Act 2018
DfE	Keeping and Maintaining Records
JSP 440	Defence Manual of Security, Resilience and Business Continuity
LFSO 2019	The Security of Personal and Mission Critical Information
GDPR May 2018	General Data Protection Regulation
JSP 441	Managing Information in Defence (Parts 1 and 2) Part 2 Guides: Records 02 Records 05
JSP 604	Information and Communications Technology in Defence
JSP 747	Web Publishing Policy
JSP 740	MOD Acceptable Use Policy
DCS Dir 7.1.1	Data Protection
DCS Dir 3.2.3	Child Protection Record Keeping Guidance

Introduction

1. This DCS Directive complements Defence policies on records management and includes direction on records specific to Children and Young People. This document should be read in conjunction with DCS Directive 7.1.1 (Data Protection) and 7.1.5 (Child Protection Record Keeping Guidance.)

2. All DCS personnel are to follow Defence policy on the management[1] of records, as below:

a. JSP 441 Parts 1 and 2, Managing Information in Defence and supporting guidance notes;

b. JSP 747, Web Publishing Policy

c. JSP 604, Information and Communications Technology in Defence

d. JSP 740, MOD Acceptable Use Policy.

Aims

3. This document clarifies direction on the management of records within DCS and provides a sample Records Retention Schedule for adoption within the Directorate.

Scope

4. This directive applies to all records, in all electronic or physical formats or media, created, received or maintained by all personnel employed within DCS, including MOD schools/settings overseas.

5. As required, Queen Victoria School follows the Scottish Government's statutory requirements for the management of records and this Directive where using MOD information systems.

General

6. Records are defined in Defence as any information created, received or maintained in the following formats:

a. Physical, for example, a document, letter, certificate, image, notes

b. Electronic, for example, email, web information, voice/video recording

7. To compliance with the Data Protection Principles laid out in the Data Protection Act 2018 (DPA 18), all information must be:

a. Legally held and used;

b. Correctly labelled and stored;

c. Readily available in a helpful format to those who should have access to it;

d. Securely protected from those who should not have access to it;

e. Preserved for an appropriate period of time.

8. Effective records management begins by ensuring that the right information is captured, labelled correctly and stored in an appropriate shared area with the required access

[1] The term 'management' covers normal processing, retention and disposal of records.

permissions. Declaring information as a record provides assurance that it will be appropriately retained and protected against amendment or premature disposal.

9. **All DCS personnel are to complete the mandatory online Defence Information Management Passport (DIMP) training**.

10. As a general principle, we should declare as records information which has corporate value (short or long term), including:

a. that which contributes to discussion or decision, such as policy documents, reports, reviews, guides, as well as any correspondence sent externally;

b. that produced regularly as part of an administrative or operational process, such as minutes, meeting papers, data returns, reports, Memoranda of Understanding, and audits.

11. Important information must be saved as records, in particular:

a. any material that would be regarded as a significant Historical Record, which will include the documents summarised in the last paragraph of this section;

b. records retained for Legal or Audit Purposes, including legal, finance and accounting records, contracts and agreements (noting that these may need to be retained in hard copy as well).

Responsibilities

12. All personnel are responsible for maintaining records and record keeping systems in accordance with Defence policy (JSP 441):

a. keeping accurate official records;

b. preparing records correctly for storage. Self-modifying fields (such as those that display ‘current date’ whenever the file is opened) should be replaced by fixed data as at the time the record is being created. Records should not be encrypted, compressed, password protected, or in any condition that will make them difficult to access by authorised people;

c. storing records correctly in the right shared areas in accordance with unit guidance. Electronic records must not be stored offline on media such as CD, DVD, portable drives, etc.

13. Personnel specifically responsible for records management are to:

a. Provide guidance for good records management practice;

b. Promote compliance with policy by routinely checking that records are securely stored and appropriately accessible;

c. Ensure that records are transferred, stored and disposed of appropriately and in accordance with MOD and Govt (UK wide) guidelines.

14. **MOD schools/settings are responsible for the creation and maintenance of school level records management procedures and must also be able to demonstrate their compliance with it. Where an external contract is used to process records, this will need to be included in the school retention schedule** (for example, One Team Logic's 'MyConcern' software use for child protection and safeguarding records).

15. Labour Support Units/LEC Pay and Personnel Offices, at local overseas Commands are responsible for managing records of locally employed civilians (LECs).

16. The MOD Departmental Record Officer (DRO) is to fulfil the role as published by The National Archives (TNA), and in particular is responsible for:

a. ensuring MOD information is managed from the point of creation until it is destroyed or transferred;

b. selecting information for permanent preservation in accordance with TNA policy and guidance;

c. transferring selected records to TNA.

17. Defence Business Services (DBS) is responsible to the Departmental Records Officer for:

a. managing the MOD's archives, either directly or through a specialist supplier;

b. reviewing records, selecting important records for transfer to TNA and disposing of all material appropriately when no longer required.

Personnel Records

18. Personnel files and training records (including misconduct and working time records) should normally be retained for 6 years after employment ceases. However, records should be retained until the adult reaches retirement, or for 10 years (if this is the longer period) where any of the following concerns are identified:

a. Behaviour of an adult working with children where s/he behaved in a harmful way towards a child (actual harm or potential to harm);

b. Adult possibly committed a criminal offence against or related to a child;

c. Adult behaved towards a child in a manner that indicated s/he was unsuitable to work with children.

19. On closing a MOD school/setting, personnel records are to be managed in accordance with MOD guidelines. Physical records are to be transferred to Defence Business Services and a schedule of records held at HQ DCS (MOD Schools). Electronic records are to be retained in accordance with MOD guidelines.

20. All records on Local Employed Civilians (LEC) files are the property of Local Support Units.

21. **Records held by CEAS.** Records on Service families retained by CEAS are processed as below:

a. SEND records are processed and retained separately and are to be transferred to TNT and retained from the Date of Birth (DOB) of the child plus 26 years.

b. Case work records are processed and retained separately and are to be kept for 6 years after the last contact with the service user.

Children and Young People Records

22. **Pupil Records.** The pupil record is the primary means of charting an individual pupil's progress through the Education System and should accompany the pupil through every stage and every school attended:

a. Pupil records are to be accurate, objective and accessible. Detailed statutory guidance is accessible on the DfE GOV.UK site.

b. Where a child completes statutory education in a MOD school, the pupil record is to be transferred to the child on leaving the school. Historical records relating to pupils who have left MOD school education are to be transferred to TNT where they should be stored from DOB + 26 years.

c. MOD schools are to send a copy of their TNT transfer record to HQ DCS (FAO the iHub).

23. **Child Protection Records.** Separate direction and guidance on the management of Child Protection Records is laid out in DCS Directive 3.2.3.

24. **Education Social Work Records.** Records generated from case work by DCS's social care and educational professionals, are to be processed as below and disposed of securely unless subject to a legal hold:

a. All case work that relates to child welfare (including referrals and non-referrals) should be kept for 6 years after the last contact with the service;

b. One-off consultation records may be destroyed a year after the CYP concerned ceases to use DCS services.

25. **Special Educational Needs and Disability (SEND) Records.** SEND records are retained from DOB of the pupil plus 26 years and disposed of securely unless subject to a legal hold. DCS may choose to keep SEND files for a longer period to defend itself in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented. The normal processing of SEND records is conducted as below:

a. The normal processing of SEND records, including those created in support of the MOD's Assessment of Supportability Overseas, is undertaken by the Educational Psychologists and Advisory Specialists (EPAS) team;

b. SEND files (including advice and information provided to parents), reviews and Individual Education Plans (IEP) are normally transferred by the MOD school to the receiving school – the receiving school is then responsible for normal processing of these records;

c. Where a child completes compulsory mainstream schooling in a MOD school, these records are to be transferred to TNT.

Retention Schedule

26. The principle underpinning retention of records as directed through the DPA is that: 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

27. The MOD's Data Protection policy provides guidance on retention periods for personal information,[2] and when deciding how long to retain information, personnel should consider whether information is affected by:

a. legislation which directs a statutory retention period;

b. A limitation period, for example keeping a contract for at least the length of time that a claim could be brought against it;

28. All DCS functional areas, including MOD schools are required to maintain a retention schedule which sets out the normal processing of records; the length of time a record series needs to be kept and the action required when it is of no further administrative use. Detailed guidance on the types of records held within Defence establishments and their recommended retention periods is accessed at JSP 441 Part 2 – Guide Records 01 and 05.

29. The retention schedule should be used by personnel to manage current record keeping systems and to inform the creation of new record keeping systems. The schedule references a record series regardless of the media in which they are stored (paper or electronic). DCS personnel are to adapt and populate the model Retention Schedule at Annex A.

30. Managing records against the retention schedule is deemed to be "normal processing" under statute (DPA and FOIA) and once an FOI request is received or a legal hold imposed, records disposal relating to the request or legal hold must be stopped.

31. Retention schedules are to be regularly reviewed and amended to include any new record series and remove obsolete ones.

Disposal

32. Not all records are of long-term value and worthy of permanent preservation. When a file is closed the records within should be reviewed by the Information Asset Owner and a decision on their long-term value must be made. All records are to be securely disposed of and child protection records must be shredded. Detailed direction is accessed at 2019DIN05-002: Records Management – The 20 Year Rule.

[2] MOD Data Protection Guidance Note 5

Transfer to Archives

33. Registered documents that need to be retained should be sent to MOD Main Archives for records classified up to SECRET or to MOD Sensitive Archives for material classified above SECRET. Detailed guidance is accessed at JSP 441 Part 1.

34. Records of historical interest from MOD schools may be archived. Schools are to contact the BFES SCEA Hon Archivist for consideration of permanent preservation. Schools should contact HQ DCS (MOD Schools) for contact details.

Subject Access Requests (SAR)

35. Effective information and records management is crucial to being able to process Freedom of Information Act and Data Protection Act requests. Both Acts require organisations to search all their information and data holdings for anything within the scope of the request, then review the content in line with the respective Act and consider any justifiable exemptions ahead of releasing any documents.

36. It is therefore crucial to have identifiable locations where DCS documents are being held, to label them appropriately and to have an electronically-searchable index to enable swift and effective searches as required.

37. This is especially important for large holdings of hardcopy (physical) files, as both FOIs and SARs have mandated timescales to complete the process in (FOI - 20 working days. SAR - 30 calendar days).

38. Both Acts recognise where information has been appropriately destroyed after their retention period and utilise an ‘information not held’ template reply.

Annex A – Retention Schedule

This model Retention Schedule provides examples of retention periods and is not exhaustive. The template should be adapted for use by each DCS functional area and MOD school (overseas and QVS) and should detail the normal processing of records.

Serial	File Description	Statutory Provisions	Minimum Retention Period	Action at end of record life
1.	Correspondence (email, physical record)	Limitation Act 1980	Termination of Employment + 6 years or longer where subject to investigation.	Secure Disposal
2.	Personnel Administration	Limitation Act 1980	Retain 1 year after closure of file.	Secure Disposal
3.	Personnel Records	Limitation Act 1980	Termination of Employment + 6 years. For pension requirements, DOB + 100 or DOB + 5 from last action. Personal security records are kept only for as long as required.	Secure Disposal
4.	Pupil Educational Records	The Education (Pupil Information) (England) Regulations Limitation Act 1980	Primary: retain whilst child remains in the primary school Secondary: DOB + 25 years[3]	File should follow pupil Secure Disposal
5.	Child Protection Records	"Keeping children safe in education" statutory guidance	Records held on the Pupil File should be in a sealed envelope and retained for the same period as the pupil file. Records held in separate files should be retained from DOB + 25 years then reviewed.	Secure Disposal – these records must be shredded
6.	Special Educational Needs	Limitation Act 1980 Education Act 1996 SEND Act 2001	DOB + 26 years Records may be retained for longer (defence against 'failure to provide sufficient education case) and this needs to be documented.	Secure Disposal

[3] 18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school

Serial	File Description	Statutory Provisions	Minimum Retention Period	Action at end of record life
7.	Education Social Work Case Records	"Keeping children safe in education" statutory guidance Limitation Act 1980	Education Social Work Records should be retained for 6 years unless subject to legal hold. One-off consultation records may be destroyed a year after the CYP concerned ceases to use DCS services.	Secure Disposal
8.	Allegation of a Persochild protection nature against personnel	"Keeping children safe in education" statutory guidance	Until the person's retirement or 10 years from the date of the allegation, whichever is the longer period and then reviewed. Allegations found to be malicious should be removed.	Secure Disposal
9.	Complaints (in all media)	Limitation Act 1980 "Keeping children safe in education" statutory guidance	6 years after employment ceases or longer (see allegations) where: There are concerns about people who work with CYP; Employee has breached the code of conduct.	Secure Disposal
10.	CEAS case work	"Keeping children safe in education" statutory guidance Limitation Act 1980	Minimum period of 1 year after the child/adult concerned ceases to use DCS services. A longer period may be required where the subject of case work is evidenced in safeguarding referrals, complaints, allegations and investigations.	Secure Disposal
11.	MOD school management records	Limitation Act 1980 Education Regulations 2002 Education Act 2002	General operational management: current year + 6 years Date of report + 10 years Date of meeting + 6 years	Secure Disposal
12.	Health and Safety	Limitation Act 1980	Records pertaining to personal injury actions should be kept for 40-60 years.	Secure Disposal
13.	Finance Budget Structure		N/A	